(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11196392 A**

(43) Date of publication of application: **21 . 07 . 99**

(51) Int. Cl **H04N 7/08**
H04N 7/081
G06F 13/00
G06T 1/00
G09C 5/00
H04N 1/387

(21) Application number: **10000874**

(22) Date of filing: **06 . 01 . 98**

(71) Applicant: **NTT DATA CORP**

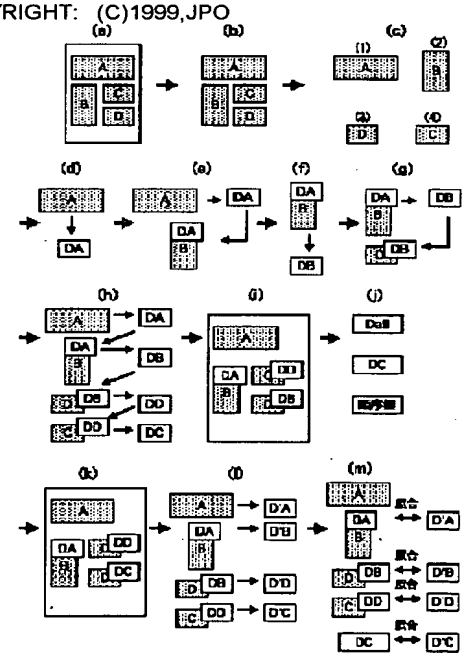
(72) Inventor: **KONISHI KAZUYA**
YAMAOKA MASATERU

(54) **METHOD FOR DETECTING FALSIFICATION OF ELECTRONIC IMAGE AND FALSIFICATION DETECTION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the falsification detection method where a falsified position of an electronic image is located.

SOLUTION: A distributor side generates transmission digests DA, DB, DD, DC based on division images A-D that denote sequenced electronic image divisions according to each area, the digests are imbedded to the division images A-D as shown in figure (h), and the division images A-D are built up in a form of the original image to reconfigure the entire image. Then an entire authentication digest generated from this entire image is distributed together with the entire image. A receiver side generates an entire image collation digest from the distributed entire image and compares it with the distributed entire image authentication digest to discriminate presence of an entirely falsified part. In the case that an entirely falsified part is in existence, reception digests D'A, D'B, D'D, D'C are generated and sequentially moved down from division images A-D read from the entire image according to the sequencing as above, and they are sequentially compared with the transmission digests sequentially to detect the presence of falsification for each division area.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－196392

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	7/08		Ｈ０４Ｎ	7/08	Ｚ
	7/081		Ｇ０６Ｆ	13/00	３５１Ｇ
Ｇ０６Ｆ	13/00	３５１	Ｇ０９Ｃ	5/00	
Ｇ０６Ｔ	1/00		Ｈ０４Ｎ	1/387	
Ｇ０９Ｃ	5/00		Ｇ０６Ｆ	15/66	Ｂ

審査請求　未請求　請求項の数８　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平10－874

(22)出願日　平成10年(1998)１月６日

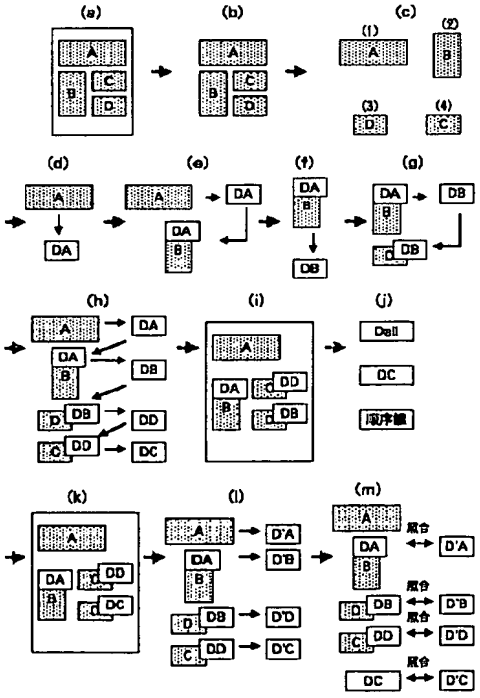
(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　小西　一也
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　山岡　正輝
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　電子画像の改竄検出方法及び改竄検出システム

(57)【要約】

【課題】　電子画像の改竄位置の特定が可能な改竄検出方法を提供する。

【解決手段】　配信側で、電子画像を領域毎に順序付けた分割画像Ａ～Ｄから送信用ダイジェストＤＡ，ＤＢ，ＤＤ，ＤＣを作成し、それぞれ次領域の分割画像へ順次繰り下げて埋め込んだ後、各分割画像Ａ～Ｄを元の電子画像の形態に組み上げて全体画像を再構成する。その後、この全体画像から作成した全体認証用ダイジェストを全体画像と共に配信する。受信側では、配信された全体画像から全体照合用ダイジェストを作成し、これを配信された全体認証用ダイジェストと比較照合して全体的な改竄の有無を判定する。全体的な改竄がある場合は、全体画像を上記順序付けに従って読み出した分割画像Ａ～Ｄから順次受信用ダイジェストＤ´Ａ，Ｄ´Ｂ，Ｄ´Ｄ，Ｄ´Ｃを作成して順次繰り下げた上で、送信用ダイジェストと順次比較照合し、領域毎の改竄の有無を検出する。



1

【特許請求の範囲】

【請求項１】　配信対象となる電子画像に所定のダイジェストを埋め込む第１段階と、配信された電子画像から前記埋め込まれたダイジェストを読み出して配信途中での改竄の有無を検出する第２段階とを有し、

前記第１段階は、

前記電子画像から領域毎の分割画像を作成して順序付けを行い、先順の分割画像から作成した送信用ダイジェストを次順の分割画像に埋め込んで当該次順の送信用ダイジェストを作成する処理をすべての分割画像について繰り返した後、最先の分割画像及び各送信用ダイジェストが埋め込まれた分割画像を元の電子画像の形態に組み上げて全体画像を再構成し、この全体画像を、当該全体画像から作成した全体認証用ダイジェスト、前記順序付けの情報、及び、最終の分割画像から作成した送信用ダイジェストと共に配信する過程を含み、

前記第２段階は、

配信された前記全体画像から作成した全体照合用ダイジェストと、配信された前記全体認証用ダイジェストとを比較照合して全体的な改竄の有無を判定し、改竄が有ると判定できるときに、前記配信された全体画像から前記順序付けの情報に従って領域毎の分割画像を読み出し、各分割画像から順次作成した受信用ダイジェストを最先の分割画像のものから次の分割画像のものへと順次繰り下げた上で、それぞれ前記送信用ダイジェストと順次比較照合して領域別の改竄の有無を判定する過程を含むことを特徴とする、電子画像の改竄検出方法。

【請求項２】　前記第１段階は、前記最終の分割画像の送信用ダイジェストを認証用ダイジェストとし、前記第２段階は、前記最終の分割画像の受信用ダイジェストを照合用ダイジェストとして前記認証用ダイジェストとの間で比較照合することを特徴とする、請求項１記載の改竄検出方法。

【請求項３】　前記送信用ダイジェスト、前記受信用ダイジェスト、前記全体認証用ダイジェスト、及び前記全体照合用ダイジェストが、各分割画像に対して一意に定まる情報であることを特徴とする請求項１または２記載の改竄検出方法。

【請求項４】　前記送信用ダイジェスト、前記受信用ダイジェスト、前記全体認証用ダイジェスト、及び前記全体照合用ダイジェストを、それぞれ元の画像に一方向ハッシュ関数を適用することにより作成することを特徴とする請求項１または２記載の改竄検出方法。

【請求項５】　前記一意に定まる情報が当該電子文書の著作権情報を含むものであることを特徴とする請求項４記載の改竄検出方法。

【請求項６】　受信した電子画像に埋め込まれたダイジェストに基づいて当該電子画像の改竄の有無を検出する手段を備えた受信装置宛の送信用情報を作成する装置であって、

2

所定の電子画像を部分領域毎の分割画像に分割する領域分割手段と、

個々の前記分割画像に対して順序付けを行う順序付け手段と、

前記順序付けの情報に従って先順の分割画像についての送信用ダイジェストが埋め込まれた分割画像または最先の分割画像から当該順の送信用ダイジェストを作成してそれぞれ次順の分割画像に順次埋め込む手段と、

最先の分割画像及び前記送信用ダイジェストが埋め込まれた分割画像を元の電子画像の形態に組み上げる画像再構成手段と、

前記組み上げられた電子画像から全体認証用ダイジェストを作成する全体認証用ダイジェスト作成手段と、

作成された全体認証用ダイジェストを、少なくとも前記組み上げられた電子画像及び前記順序付けの情報と共に前記送信用情報として保持する情報保持手段と、

を有することを特徴とする情報埋め込み装置。

【請求項７】　請求項６記載の情報埋め込み装置で作成された前記送信用情報を受信して配信過程の改竄の有無を検出する装置であって、

前記組み上げられた電子画像から全体照合用ダイジェストを作成する全体照合用ダイジェスト作成手段と、

作成された前記全体照合用ダイジェストと配信された前記全体認証用ダイジェストとを比較照合して全体的な改竄の有無を判定する第１判定手段と、

全体的な改竄が有ると判定できるときに、前記組み上げられた電子画像から前記順序付けの情報に従って領域毎の分割画像を読み出し、各分割画像から順次受信用ダイジェストを作成する受信用ダイジェスト作成手段と、

各分割画像の受信用ダイジェストをそれぞれ次順の分割画像へと順次繰り下げた上で、それぞれ前記送信用ダイジェストと順次比較照合することで領域毎の改竄の有無を判定する第２判定手段を有することを特徴とする改竄検出装置。

【請求項８】　請求項６記載の情報埋め込み装置と、請求項７記載の改竄検出装置とを通信回線で接続して成る改竄検出システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文書それ自体や文書内の図、表、パラグラフ等を電子化した、配信可能な電子画像（電子文書）の部分的な改竄の有無及び改竄位置を検出する技術に関する。

【０００２】

【従来の技術】近年、不特定多数の利用者がアクセスできるインターネット等のオープンなネットワークを通して様々な電子画像を配信及び受信する機会が増加している。ところが、こうしたオープンなネットワーク環境では、不特定多数の者が利用するため、配信途中で電子画像が第三者によって改竄され、受信者が改竄されたこと

に気付かない場合も想定される。そこで、配信された電子画像が送り手から送り出されたものと同一であるか否か、或いは送り手が正当者であるか否かの確認を受信側でチェックする電子認証の仕組みが必要とされる。

【０００３】図７は、従来の電子認証の手順の概要を示した説明図である。配信側では、オリジナルの電子画像に対してハッシュ関数によるデータ圧縮を行ってダイジェストを作成した後、作成されたダイジェストを送り手による秘密鍵で暗号化する。そして、オリジナルの電子画像及び暗号化されたダイジェストをネットワークを通して受信側に配信する。受信側では、ネットワークより受信した電子画像に対してハッシュ関数によるデータ圧縮を行ってダイジェストを作成すると共に、暗号化されたダイジェストに対して送り手の公開鍵による復号化を行ってダイジェストを復号する。そして、オリジナルの電子画像から作成したダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば改竄が行われていないと判定し、逆に、異なっていれば改竄が行われていると判定する。

【０００４】ところで、上述のようにして電子認証を行う場合、配信側では、オリジナルの電子画像及び暗号化されたダイジェストの２種類のデータを受信側へ配信する必要があるが、電子画像が大量の場合には、ネットワークを通して配信する際に、どの電子画像に対してどのダイジェストが対応しているのかを配信側で適切に管理するためのデータ管理手段が別途必要になる。このようなデータ管理手段として、従来、データハイディング手法、すなわち、例えば電子文書の著作権情報をダイジェストとして暗号化し、このダイジェストをオリジナルの電子画像中に人間の目では視認できないように秘匿に埋め込んでおき、このダイジェストを必要なときに復号化して読み出す手法が採用されている。

【０００５】なお、電子画像に対する情報の埋め込み方法を採用した周知技術としては、電子画像を周波数領域に展開して特定の周波数成分に処理を施す方法を示した技術（文献「中村，小川，高嶋：ディジタル画像の著作権保護のための周波数領域における電子透かし方式，The 1997 Symposium on Cryptography and InformationSecurity-26A」に開示された技術）や、電子画像を構成する各画素の濃度値等に直接処理を施す方法を示した技術（文献「滑水，沼尾，森本：ピクセルブロックによる静止電子画像データハイディング，情報処理学会第５３回全国大会2-257」に開示された技術）等が挙げられる。

【０００６】

【発明が解決しようとする課題】上述のデータハイディング手法を採用することにより、例えば、ネットワークを通して配信された電子画像から著作権情報等を受信者が容易に確認できるので、個々の電子画像とダイジェストとの関係の管理が容易になるほか、電子画像上に別途著作権表示をする必要が無くなるので、オリジナルの電子画像のまま保つことができる等の長所がある。

【０００７】しかしながら、従来のデータハイディング手法では、配信途中で電子画像が改竄されたことを受信側で発見できても、電子画像中のどの部分が改竄されたかを特定することができないという問題があった。

【０００８】そこで本発明の課題は、改竄部分の特定が可能な電子画像の改竄検出方法を提供することにある。本発明の他の課題は、上記改竄検出方法を適用した改竄検出システム及びその構成装置を提供することにある。

【０００９】

【課題を解決するための手段】上記課題を解決する本発明の改竄検出方法は、配信対象となる電子画像に所定のダイジェストを埋め込む第１段階と、配信された電子画像から前記埋め込まれたダイジェストを読み出して配信途中での改竄の有無を検出する第２段階とを有する。第１段階は、前記電子画像から領域毎の分割画像を作成して順序付けを行い、先順の分割画像から作成した送信用ダイジェストを次順の分割画像に埋め込んで当該次順の送信用ダイジェストを作成する処理をすべての分割画像について繰り返した後、最先の分割画像及び各送信用ダイジェストが埋め込まれた分割画像を元の電子画像の形態に組み上げて全体画像を再構成し、この全体画像を、当該全体画像から作成した全体認証用ダイジェスト、前記順序付けの情報、及び、最終の分割画像から作成した送信用ダイジェストと共に配信する過程を含み、第２段階は、配信された前記電子画像から作成した全体照合用ダイジェストと、配信された前記全体認証用ダイジェストとを比較照合して全体的な改竄の有無を判定し、改竄が有ると判定できるときに、前記配信された電子画像から前記順序付けの情報に従って領域毎の分割画像を読み出し、各分割画像から順次作成した受信用ダイジェストを最先の分割画像のものから次の分割画像のものへと順次繰り下げた上で、それぞれ前記送信用ダイジェストと順次比較照合して領域別の改竄の有無を判定する過程を含むことを特徴とする。なお、前記第１段階では、前記最終の分割画像の送信用ダイジェストを認証用ダイジェストとし、前記第２段階は、前記最終の分割画像の受信用ダイジェストを照合用ダイジェストとして、前記認証用ダイジェストとの間で比較照合するようにする。

【００１０】上記他の課題を解決する本発明の改竄検出システムは、情報埋め込み装置と改竄検出装置とを通信回線を介して接続して構成される。情報埋め込み装置は、受信した電子画像に埋め込まれたダイジェストに基づいて当該電子画像の改竄の有無を検出する手段を備えた受信装置宛の送信用情報を作成する装置であって、所定の電子画像を部分領域毎の分割画像に分割する領域分割手段と、個々の前記分割画像に対して順序付けを行う順序付け手段と、前記順序付けの情報に従って先順の分割画像についての送信用ダイジェストが埋め込まれた分割画像または最先の分割画像から当該順の送信用ダイジ

ェストを作成してそれぞれ次順の分割画像に順次埋め込む手段と、最先の分割画像及び前記送信用ダイジェストが埋め込まれた分割画像を元の電子画像の形態に組み上げる画像再構成手段と、前記組み上げられた電子画像から全体認証用ダイジェストを作成する全体認証用ダイジェスト作成手段と、作成された全体認証用ダイジェストを、少なくとも前記組み上げられた電子画像及び前記順序付けの情報と共に前記送信用情報として保持する情報保持手段と、を有することを特徴とする。

【００１１】また、改竄検出装置は、前記組み上げられた電子画像から全体照合用ダイジェストを作成する全体照合用ダイジェスト作成手段と、作成された前記全体照合用ダイジェストと配信された前記全体認証用ダイジェストとを比較照合して全体的な改竄の有無を判定する第１判定手段と、全体的な改竄が有ると判定できるときに、前記組み上げられた電子画像から前記順序付けの情報に従って領域毎の分割画像を読み出し、各分割画像から順次受信用ダイジェストを作成する受信用ダイジェスト作成手段と、各分割画像の受信用ダイジェストをそれぞれ次順の分割画像へと順次繰り下げた上で、それぞれ前記送信用ダイジェストと順次比較照合することで領域毎の改竄の有無を判定する第２判定手段を有することを特徴とする。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して詳細に説明する。

（第１実施形態）まず、本発明の改竄検出方法の実施の形態を図１に従って説明する。ここでは、配信対象となる電子画像にダイジェストを埋め込む配信側の処理と、埋め込まれたダイジェストに基づいて配信途中での改竄の有無を検出する受信側の処理を中心に説明する。

【００１３】配信側では、以下のようにしてダイジェストの埋め込みを行う。最初に、対象となる電子画像を例えば４つの部分領域に領域分割する。分割された領域の画像をそれぞれ分割画像Ａ～Ｄとする（図１（ａ））。次に、各分割画像Ａ～Ｄを抽出して（図１（ｂ））、それぞれ順序番号(1)～(4)を付与する（図１（ｃ））。図示の例では、分割画像Ａが最先で、以後、分割画像Ｂ，Ｄ，Ｃの順に順序付けされている。その後、順序番号(1)の分割画像Ａに一方向ハッシュ関数を適用して送信用ダイジェストＤＡを作成し（図１（ｄ））、これを順序番号(2)の分割画像Ｂへ埋め込む（図１（ｅ））。次に、送信用ダイジェストＤＡが埋め込まれた順序番号(2)の分割画像Ｂに一方向ハッシュ関数を適用して送信用ダイジェストＤＢを作成し、これを順序番号(3)の分割画像Ｄへ埋め込む（図１（ｇ））。この処理を最終の順序番号(4)の分割画像Ｃまで同様に繰り返す（図１（ｈ））。最終の分割画像Ｃから作成した送信用ダイジェストＤＣについては、後の処理で認証用ダイジェストとして用いるために保存しておく。

【００１４】その後、最先の分割画像Ａと各送信用ダイジェストＤＡ，ＤＢ，ＤＤが埋め込まれた分割画像Ｂ～Ｄとを元の領域に組み上げて電子画像（便宜上、元の電子画像と区別するため、以後、全体画像と称する）を再構成すると共に（図１（ｉ））、その全体画像に一方向ハッシュ関数を適用して全体認証用ダイジェストＤａｌｌを作成する。そして、上記順序付けの情報としての順序鍵、全体認証用ダイジェストＤａｌｌ、認証用ダイジェストＤＣ、及び全体画像を受信側に配信する（図１（ｊ））。

【００１５】一方、受信側では、以下のようにして、改竄検出を行う。受信した全体画像に一方向ハッシュ関数を適用して認証照合用ダイジェストを作成し、この認証照合用ダイジェストと全体認証用ダイジェストＤａｌｌとを比較照合して全体的な改竄の有無を判定する（図１（ｋ））。両ダイジェストが一致した場合、すなわち全体的な改竄がなかった場合は、その全体画像についての所定の後続処理を行う。

【００１６】一方、全体的な改竄があった場合は、以下のようにして領域別の改竄の有無を検出する。まず、全体画像を、受信した順序鍵に従って分割し、これにより得られた分割画像から順次受信用ダイジェストＤ´Ａ，Ｄ´Ｂ，Ｄ´Ｄ，Ｄ´Ｃを作成する（図１（ｌ））。また、順序番号(2)以降の分割画像から埋め込まれている送信用ダイジェストをそれぞれ読み込んでおく。そして、順序番号(1)の分割画像Ａの送信用ダイジェストＤＡと受信用ダイジェストＤ´Ａ，順序番号(2)の分割画像Ｂの送信用ダイジェストＤＢと受信用ダイジェストＤ´Ｂ，順序番号(3)の分割画像Ｄの送信用ダイジェストＤＤと受信用ダイジェストＤ´Ｄ、順序番号(4)の分割画像Ｃについての認証用ダイジェストＤＣと照合用ダイジェストＤ´Ｃとをそれぞれ比較照合する（図１(m)）。これにより、領域別の改竄の有無の判定が可能になる。

【００１７】（第２実施形態）次に、上記改竄検出方法を適用した改竄検出システムについて説明する。この改竄検出システムは、配信装置と受信装置をそれぞれネットワークに接続して構成される。配信装置は、対象となる電子画像に上記送信用ダイジェストを付加する情報埋め込み装置を備え、受信装置には上記各種ダイジェストを用いて全体改竄検出及び領域別の改竄検出を行う改竄検出装置を備えている。

【００１８】配信装置に備えられる情報埋め込み装置は、少なくとも下記の機能を有するものである。

（１）所定の電子画像を部分領域毎の分割画像に分割する機能。

（２）個々の前記分割画像に対して順序付けを行う機能。

（３）順序付けの情報に従って先順の分割画像についての送信用ダイジェストが埋め込まれた分割画像または最

先の分割画像から当該順の送信用ダイジェストを作成してそれぞれ次順の分割画像に順次埋め込む機能。

（４）最先の分割画像及び送信用ダイジェストが埋め込まれた分割画像を元の電子画像の形態に組み上げて全体画像を再構成する機能。

（５）全体画像から全体認証用ダイジェストを作成する機能。

（６）作成された全体認証用ダイジェストを、少なくとも全体画像及び前記順序付けの情報と共に送信用情報として保持する機能。

【００１９】上記各機能を実現するため、本実施形態では、図２に示すように、画像入力部１１，画像蓄積部１２，画像出力部１３，画像再構成部１４，自動領域分割部１５，領域データ蓄積部１６，ダイジェスト作成部１７，ダイジェスト蓄積部１８，全体認証用ダイジェスト出力部１９，情報埋込部２０，認証用ダイジェスト出力部２１，手動領域分割部２２，領域座標データ入力部２３，領域座標データ蓄積部２４，順序鍵作成部２５，順序鍵蓄積部２６，順序データ入力部２７，順序データ蓄積部２８，及び順序鍵出力部２９の機能ブロックを備えた情報埋め込み装置１００を構成する。この情報埋め込み装置１００は、例えばパーソナルコンピュータやワークステーション等の汎用コンピュータが記録媒体に記録された所定のプログラムを読み込んで実行することによって実現することができる。

【００２０】以下、電子画像として、１画素が８ビットで表わされる２５６階調のグレースケールビットマップ形式の画像を対象とし、各分割画像から得られるダイジェストが８ビットであるものとして、情報埋め込み装置１００の使用手順と上記各部１１～２９の動作を説明する。なお、画像蓄積部１２の蓄積内容や画像処理の過程は、図示しない表示装置の画面上に表示され、随時モニタできるようになっている。

【００２１】まず、図示しないメモリにファイルされた電子画像から改竄位置の特定を可能にしたいものを画像入力部１１で読み込んで画像蓄積部１２に保存させておく。この情報埋め込み装置１００は、電子画像の領域分割を自動で行うか、或いは手動で行うかを利用者が適宜指定できるようになっている。自動領域分割が指定された場合、自動領域分割部１５は、画像蓄積部１２に保存されている電子画像を、図，表，パラグラフ等の部分領域に分割し、分割画像を得る。

【００２２】図３は、領域分割の処理内容を説明するために示したものであり、同図（ａ）は黒画素数の分布グラフ、同図（ｂ）は分割される電子画像の一例である。ここでは、図３（ｂ）に示されるような電子画像に対して一定値以上の濃度値（例えば“１２８”）を持つ画素を“１”，それ未満の画素を“０”とする２値化処理をライン毎に施し、そのラインに含まれる黒画素数を通計して図３（ａ）に示されるような、縦軸が画像の縦方向

の座標値，横軸が通計した黒画素数となるグラフを作成する。このとき、例えば１０ライン以上連続して、通計した黒画素数が“０”となる位置で電子画像を分割する。更にその分割領域において全カラムの黒画素を通計して同様なグラフを作成し、例えば１０カラム以上連続して、通計した黒画素数が“０”となる位置で再分割する。このような操作を領域が分割されなくなるまで繰り返す。

【００２３】この結果、例えば最終的に図４に示されるように、８つの分割画像が抽出可能になる。これらの分割画像及びそれらの各々の位置座標（各分割画像の左上端座標等）の情報は、領域データ蓄積部１６に保存される。また、各分割画像の位置座標，幅，高さの情報は、領域座標データ蓄積部２４に保存される。

【００２４】一方、手動領域分割が指定された場合、利用者は、電子画像を表示装置のモニタ画面で見ながらマウス等の操作により分割したい領域を表す領域座標データを領域座標データ入力部２３に入力することになる。この場合、その領域の位置座標，その幅，高さの情報を含む領域座標データが領域座標データ蓄積部２４に保存され、この領域座標データに基づいて手動領域分割部２２が、電子画像を分割して分割画像を抽出する。

【００２５】その後、利用者は、画像蓄積部１２に保存されている電子画像と領域座標データ蓄積部２４に保存されているデータとを参考にして、マウス等の操作により、各分割画像に対する順序データ（上述の順序番号）を順序データ入力部２７に入力する。この順序データは、順序データ蓄積部２８及び領域データ蓄積部１６に保存される。

【００２６】ダイジェスト作成部１７では、領域データ蓄積部１６に保存されている分割画像に対して一方向ハッシュ関数を適用してデータ圧縮を行うことで、送信用ダイジェストを作成し、これをダイジェスト蓄積部１８に保存させる。例えば図５に示されるように、個々の分割画像を縦横の各方向に４等分して総計１６個の画素ブロックのビットマップイメージを作成し、各画素ブロックにおける全画素の濃度値の合計を算出し（ここでは１７２９ビット）、その合計を２５６で除した剰分（ここでは１９３）を送信用ダイジェストとして扱う。

【００２７】情報埋込部２０は、ダイジェスト蓄積部１８に保存されている最先の分割画像についての送信用ダイジェストを次の分割画像へ埋め込む。また、最先の分割送信用ダイジェストが埋め込まれた分割画像をダイジェスト作成部１７に送って送信用ダイジェストを作成させ、これにより得られた送信用ダイジェストをさらに次の分割画像に埋め込む。これを最終の分割画像に先順の送信用ダイジェストを埋め込むまで繰り返す。最終の分割画像の送信用ダイジェストについては、これを認証用ダイジェストとするため、そのままダイジェスト蓄積部１８に保存しておく。

【００２８】ここでの埋め込みは、例えば上述した公知文献「清水，沼尾，森本：ピクセルブロックによる静止全体画像データハイディング，情報処理学会第５３回全国大会2-257」に開示された技術を応用することで実現可能である。具体的に言えば、まず、領域画像を横方向から見た場合の４個の画素ブロックを左側と右側の２個ずつの組に分けて、総計１６個の画素ブロックから８個の画素ブロック対を作成し、各画素ブロック対における全画素の濃度値の分散値を比較する。比較の結果、左側ブロックの分散値が右側ブロックの分散値以上である場合、この画素ブロック対は、ビット値“０”という情報を示しており、左側ブロックの分散値が右側ブロックの分散値未満である場合、この画素ブロック対は、ビット値“１”という情報を示しているとする。ここで、画素ブロック対を左上から右下の順に見たときの各画素ブロックの各ビット値情報を埋め込む情報と照合し、その照合結果として埋め込む情報と合致しない画素ブロック対があれば、その画素ブロック対の各画素ブロックにおいて、線形変換により平均値をそのままにして分散値のみを入れ替える処理を施す。

【００２９】例えば、特定の画素ブロックＡの分散値を他の画素ブロックＢの分散値と入れ替える場合、新しい画素ブロックＡの濃度値Ｎは、その画素ブロックＡでの全画素の濃度値の平均値をＭａとした場合、「Ｎ＝Ｍａ＋（画素ブロックＡの濃度値－Ｍａ）×画素ブロックＢの分散値／画素ブロックＡの分散値」なる関係式より求めることができる。

【００３０】画像再構成部１４では、順序データ蓄積部２８からの順序データに従って領域データ蓄積部１６に保存されている各分割画像を各々の位置座標の情報を用いて元の電子画像の形態に組み上げて全体画像を再構成し、これを画像蓄積部１２に保存させる。この後、ダイジェスト作成部１７は、画像蓄積部１２に保存されている全体画像に対して一方向ハッシュ関数を適用してデータ圧縮を行うことで、全体認証用ダイジェストを作成し、これをダイジェスト蓄積部１８に保存させる。

【００３１】順序鍵作成部２５では、順序データ蓄積部２８に保存されている順序データと領域座標データ蓄積部２４に保存されているデータとに基づいて順序鍵を作成し、これを順序鍵蓄積部２６に保存させる。

【００３２】最終的に、画像出力部１３は、画像蓄積部１２に保存されている全体画像を出力する。また、全体認証用ダイジェスト出力部１９は、ダイジェスト蓄積部１８に保存されている全体認証用ダイジェストを出力する。同時に順序鍵出力部２９から順序鍵蓄積部２６に保存されている順序鍵を出力し、認証用ダイジェスト出力部２１はダイジェスト蓄積部１８に保存されている認証用ダイジェストを出力する。

【００３３】なお、送信用ダイジェストが付加された全体画像、全体認証用ダイジェスト、順序鍵、認証用ダイジェストは、図示しないメモリにファイルしておくことが可能である。また、図２に示した情報埋め込み装置１００の構成は一例であって、初めに説明した基本機能を有するものであれば他の構成であっても良い。

【００３４】次に、受信装置に備えられる改竄検出装置について説明する。この改竄検出装置は、少なくとも下記の機能を有するものである。

（１）配信された全体画像から全体照合用ダイジェストを作成する機能。

（２）作成された全体照合用ダイジェストと配信された全体認証用ダイジェストとを比較照合して全体的な改竄の有無を判定する機能。

（３）全体的な改竄が有ると判定できるときに、配信された全体画像から上記順序鍵に従って領域毎の分割画像を読み出し、各分割画像から順次受信用ダイジェストを作成する機能。

（４）各分割画像の受信用ダイジェストをそれぞれ次順の分割画像へと順次繰り下げた上で、それぞれ各送信用ダイジェストと順次比較照合することで領域毎の改竄の有無を検出する機能。

【００３５】上記各機能を実現するため、本実施形態では、図６に示すように、画像入力部３０，画像蓄積部３１，領域分割部３２，領域データ蓄積部３３，ダイジェスト作成部３４，ダイジェスト蓄積部３５，順序鍵蓄積部３６，情報検出部３７，検出情報蓄積部３８，順序鍵入力部３９，全体認証用ダイジェスト入力部４０，認証用ダイジェスト入力部４１，全体認証用ダイジェスト蓄積部４２，認証用ダイジェスト蓄積部４３，情報照合部４４，判定結果蓄積部４５，及び判定結果出力部４６を備えて改竄検出装置２００を構成する。この情報読み出し装置2-0-0は、例えばパーソナルコンピュータやワークステーション等の汎用コンピュータが、記録媒体に記録された所定のプログラムを読み込んで実行することによって実現することができる。

【００３６】改竄検出装置2-0-0における動作は、下記のとおりである。まず、画像入力部３０で、送信用ダイジェストが付加された全体画像を入力するとともに、この全体画像を画像蓄積部３１に保存させる。また、順序鍵入力部３９で入力した順序鍵を順序鍵蓄積部３６に保存させ、全体認証用ダイジェスト入力部４０で入力した全体認証用ダイジェストを全体認証用ダイジェスト蓄積部４２に保存させ、更に、認証用ダイジェスト入力部４１で入力した認証用ダイジェストを認証用ダイジェスト蓄積部４３に保存させる。

【００３７】ダイジェスト作成部３４は、画像蓄積部３１に保存された全体画像に一方向ハッシュ関数を適用してデータ圧縮を行うことで全体照合用ダイジェストを作成し、これをダイジェスト蓄積部３５に保存させる。

【００３８】情報照合部４４では、ダイジェスト蓄積部３５に保存された全体照合用ダイジェストと全体認証用

ダイジェスト蓄積部４２に保存された全体認証用ダイジェストとを比較照合し、全体的な改竄の有無を判定する。両ダイジェストが一致していれば全体的な改竄が行われていないと判定し、一致していなければ改竄が行われていると判定する。判定結果は、判定結果蓄積部４５に保存される。

【００３９】情報照合部４４において全体的な改竄が行われていると判定できる場合は、以下の手順で改竄位置の特定を行う。まず、その結果を情報照合部４４から領域分割部３２に通知する。領域分割部３２では、順序鍵蓄積部３６に蓄積された順序鍵に従って画像蓄積部３１に蓄積された全体画像を分割画像に分割して読み出して順序鍵と共に領域データ蓄積部３３に保存させる。

【００４０】次に、ダイジェスト作成部３４で、各分割画像に対して一方向ハッシュ関数を適用してデータ圧縮を行い、順次受信用ダイジェストを作成する。そして、各受信用ダイジェストをダイジェスト蓄積部３５に保存させる。また、情報検出部３７で、領域データ蓄積部３３に保存された分割画像に含まれる送信用ダイジェストを最先の分割画像のものから次の分割画像のものへと順次読み出して検出情報蓄積部３８に保存させる。

【００４１】更に、情報照合部４４で、ダイジェスト蓄積部３５に保存された受信用ダイジェストを最先の分割画像のものから次の分割画像のものへと順次繰り下げて読み出し、それぞれ検出情報蓄積部３８に保存された送信用ダイジェストと比較照合する。最終の分割画像の受信用ダイジェストについては、これを照合用ダイジェストとして、認証用ダイジェスト蓄積部４３に蓄積された認証用ダイジェストと比較照合する。それぞれのダイジェストが一致していれば各分割画像は改竄されていないことになり、相違していれば該当する分割画像は改竄されていることになる。すべての分割領域が改竄されていない結果になった場合は、領域分割時に、部分領域として選択されなかった領域が改竄されていたことを意味する。

【００４２】何れにせよ、この場合も先の全体画像に関する改竄の有無の判定結果と同様に、その比較照合の結果は、順序鍵と共に判定結果蓄積部４５に保存された後、判定結果出力部４６から出力される。

【００４３】なお、図６に示した改竄検出装置２００の構成も一例であって、初めに説明した基本機能を有するものであれば他の構成であっても良い。

【００４４】本発明の実施形態は、以上のとおりであるが、本発明は、必ずしも上記例に限定されるものではなく、種々の形態での実施が可能である。例えば、上記説明は、一方向ハッシュ関数を適用した、画像の画素濃度値に基づく各種ダイジェストの作成、及び個々の画像を更に分割したブロック間の画素濃度値の分散値の比較による埋め込みの例であるが、本発明の改竄検出が可能になる形態であれば、他の手法でダイジェストを作成しても良い。

【００４５】

【発明の効果】以上の説明から明らかなように、本発明によれば、電子画像が改竄されていることを確認した上で電子画像中のどの位置が改竄されたのかを領域別に特定することができるという特有の効果がある。また、順序付けの情報を配信しているため、この順序付けの情報を持たない利用者は改竄位置を特定できないため、利用者へのサービス限定を図ることが可能になる。

【図面の簡単な説明】

【図１】（ａ）～（ｍ）は、本発明の電子画像の改竄検出方法の処理概要及び手順を示した説明図。

【図２】本実施形態の情報埋め込み装置のブロック構成図。

【図３】本実施形態の情報埋め込み装置における電子画像の領域分割処理を説明するための図で、（ａ）は黒画素数のグラフに関するもの，（ｂ）は分割に供される全体画像に関するものである。

【図４】図３で説明した領域分割処理を経て得られた分割画像を組み上げた全体画像の説明図。

【図５】本実施形態の情報埋め込み装置におけるダイジェスト作成の説明図。

【図６】本実施形態の改竄検出装置のブロック構成図。

【図７】従来の電子認証の手順を示した説明図。

【符号の説明】

１１，３０　画像入力部
１２，３１　画像蓄積部
１３　画像出力部
１４　画像再構成部
１５　自動領域分割部
１６，３３　領域データ蓄積部
１７，３４　ダイジェスト作成部
１８，３５　ダイジェスト蓄積部
１９　全体認証用ダイジェスト出力部
２０　情報埋込部
２１　認証用ダイジェスト出力部
２２　手動領域分割部
２３　領域座標データ入力部
２４　領域座標データ蓄積部
２５　順序鍵作成部
２６，３６　順序鍵蓄積部
２７　順序データ入力部
２８　順序データ蓄積部
２９　順序鍵出力部
３２　領域分割部
３７　情報検出部
３８　検出情報蓄積部
３９　順序鍵入力部
４０　全体認証用ダイジェスト入力部
４１　認証用ダイジェスト入力部

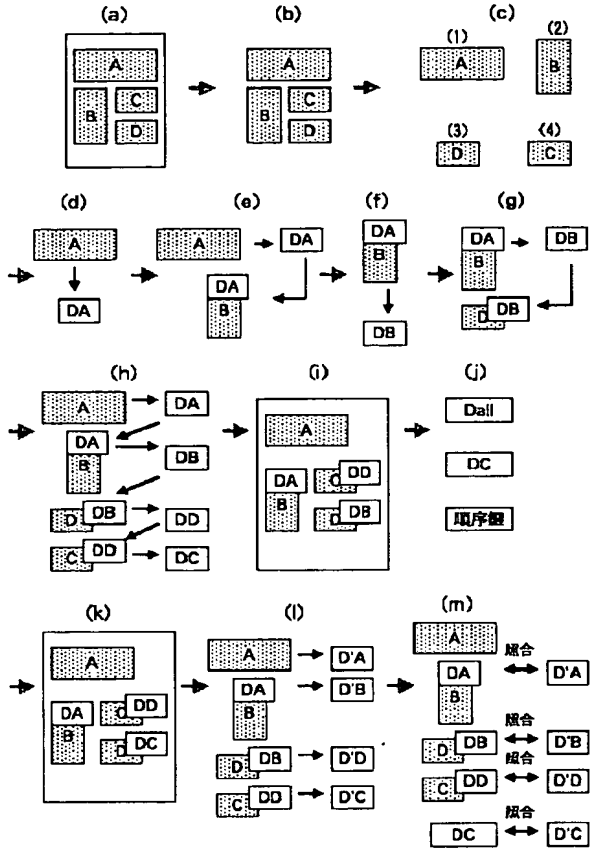
13

４２　全体認証用ダイジェスト蓄積部
４３　認証用ダイジェスト蓄積部
４４　情報照合部
４５　判定結果蓄積部

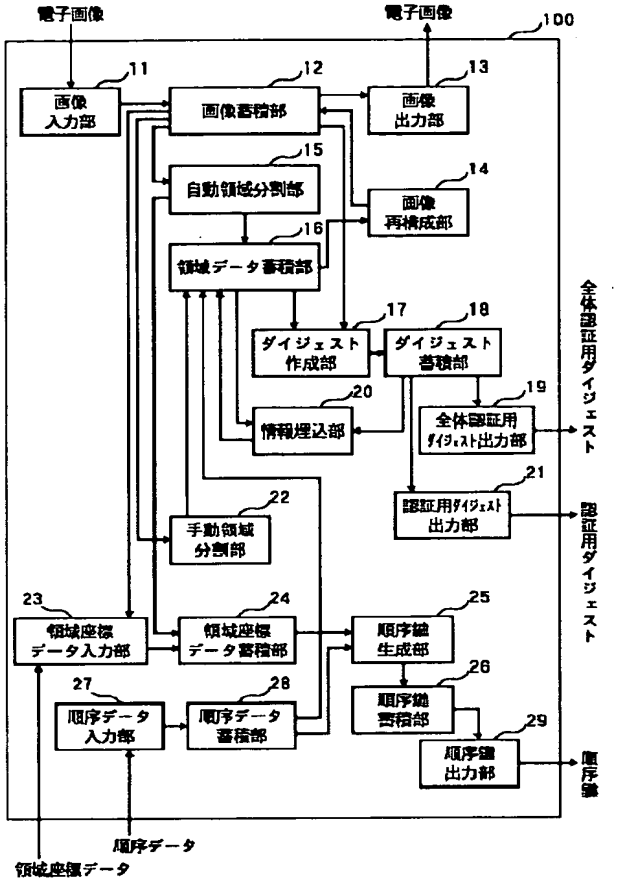
14

４６　判定結果出力部
１００　情報埋め込み装置
２００　改竄検出装置

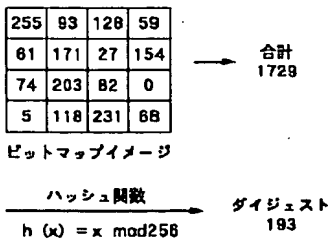
【図１】



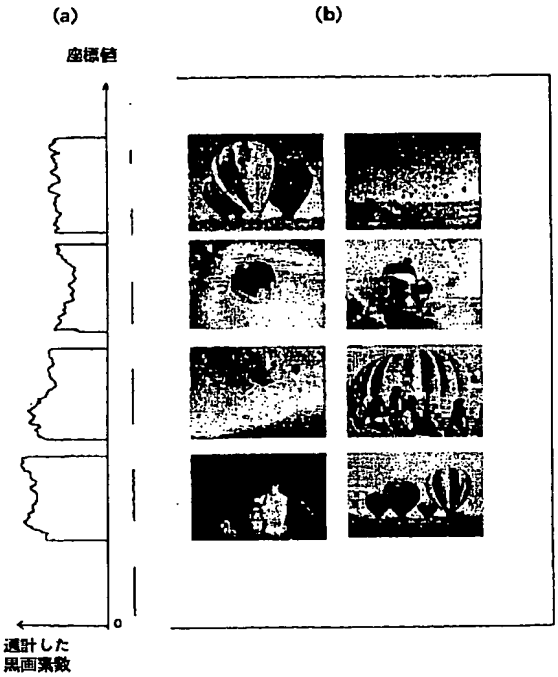
【図２】



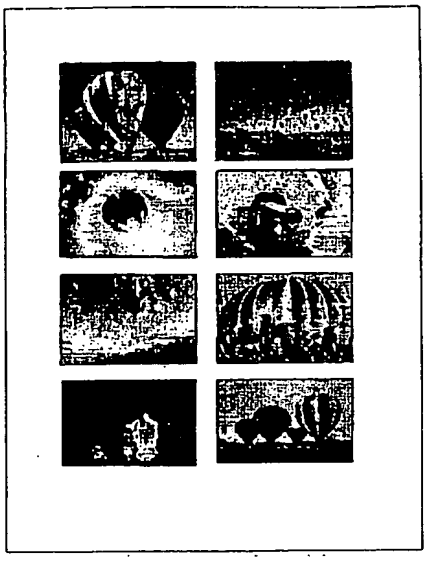
【図５】



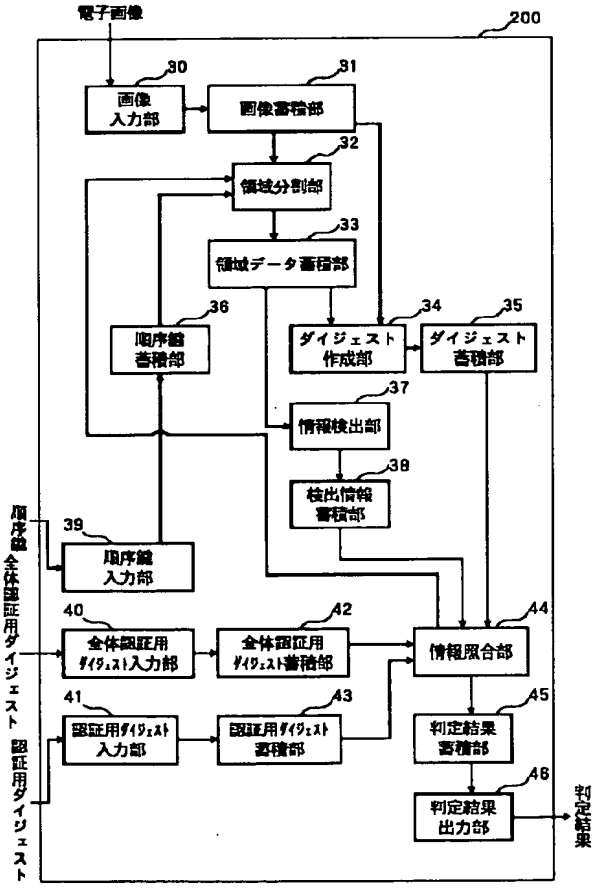
【図３】


(a)
(b)
座標値
0
過計した
黒画素数

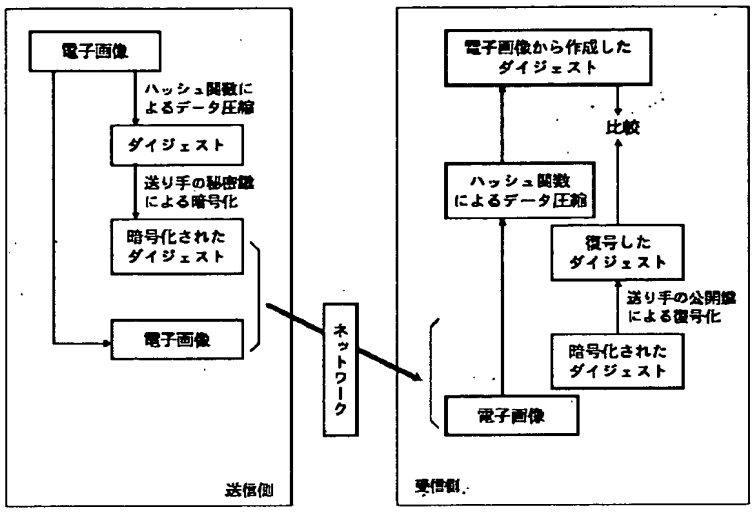
【図４】



【図６】


電子画像
200
30
画像入力部
31
画像蓄積部
32
領域分割部
33
領域データ蓄積部
34
ダイジェスト作成部
35
ダイジェスト蓄積部
36
順序線蓄積部
37
情報検出部
38
検出情報蓄積部
39
順序線入力部
順序線
全体認証用ダイジェスト
認証用ダイジェスト
40
全体認証用ダイジェスト入力部
42
全体認証用ダイジェスト蓄積部
44
情報照合部
41
認証用ダイジェスト入力部
43
認証用ダイジェスト蓄積部
45
判定結果蓄積部
46
判定結果出力部
判定結果

【図７】



フロントページの続き

(51) Int. Cl.[6]　　識別記号　　ＦＩ
　Ｈ０４Ｎ　1/387